Wireless Two-Way Electronic Mail Handheld Protection Profile

FINAL DRAFT
Version 1.0

June 2002

Prepared By: Tresys Technology

Prepared For: Department of Defense

Disclaimer

Foreword

This publication, *Wireless Two-Way Electronic Mail Handheld Protection Profile*, is issued by the National Security Agency (V34) program office as part of its program to support the next generation of wireless technologies. This protection profile is based on the "Common Criteria for Information Technology Security Evaluations, Version 2.1."

Comments on this document should be directed to: Timothy Havighurst, NSA V34. The comments should include the title of the document, the page and paragraph number, detailed comment and recommendations.

Table of Contents

List of Tables and Figures

1 Introduction

This section contains overview information necessary to allow a Protection Profile (PP) to be registered through a Protection Profile Registry. The PP identification provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference a PP. The PP overview summarizes the profile in narrative form and provides sufficient information for a potential user to determine whether the PP is of interest. The conventions section provides an explanation of how this document is organized and the glossary of terms section gives a basic definition of terms which are specific to this PP.

1.1 Identification

Title:	Wireless Two-Way Electronic Mail Handheld Protection Profile, Final Draft Version 1.0, June 2002
Authors:	Kimberly Caplan and Jandria Alexander (Tresys Technology)
Vetting Status:	Draft
CC Version	2.1
Evaluation Level:	Evaluation Assurance Level (EAL) 4
General Status:	Draft
Registration:	TBD
Keywords:	Wireless, Handheld, S/MIME, PKI, electronic mail, desktop, mail server

1.2 Protection Profile Overview

This PP is one of three profiles that are used to specify information security requirements for the wireless two-way email solution. This PP specifies security requirements for the handheld component and includes the evaluation assurance level (EAL) 4 assurance requirements, as defined by the Common Criteria. The handheld allows a traveling user to read email from their corporate-based desktop. The handheld is a single-user device used to send and receive plaintext and S/MIME mail messages over a wireless network. The handheld is part of wireless two-way email solution that provides a secure communication channel between the handheld and the mail server component. The handheld can be used in, at most, moderate risk environments to create, send, and receive signed and/or encrypted S/MIME or plaintext messages.

1.3 Conventions

Except for replacing United Kingdom spelling with American spelling, the notation, formatting, and conventions used in this PP are consistent with version 2.1 of the CC. Font style and clarifying information conventions were developed to aid the reader.

1.3.1 Operations on Components

The CC permits four component operations—assignment, iteration, refinement, and selection—to be performed on functional requirements. Refinement and iteration operations can be performed on assurance requirements. These operations are defined in CC, Part 2, paragraph 2.1.4 as

- assignment: allows the specification of an identified parameter;
- iteration: allows a component to be used more than once with varying operations;
- refinement: allows the addition of details; and
- selection: allows the specification of one or more elements from a list.

With the exception of iteration, these operations are expressed by using bolded, italicized, and underlined text.

Uncompleted *assignments and selections* are indicated by brackets ("[ ]") to set off all assignments or selections that require future action by the developer to prepare a Security Target (ST). The text " ST Assignment:" or " ST Selection:" is indicated within the brackets.

Refinements are identified by bold text.

Iterations are identified with a number inside parenthesis ("(#)"). These follow the short component and functional element names.

Explicit Requirements are allowed to create requirements should the CC not offer suitable requirements to meet the PP needs. Explicit requirements must be identified and are required to use the CC class/family/component model in articulating these requirements. The naming convention for explicit requirements is the same as that used in the CC. To ensure these requirements are explicitly identified, the ending "_EXP" is appended to the newly created short name. The newly created explicit requirements are integrated with the CC requirements and shown in bold text. The rationale for creating a requirement is provided in Section 6.2.6 Explicit Requirements Rationale.

Table 1 Functional Requirements Operation Conventions illustrates the operations as they are used in this PP.

Table 1 Functional Requirements Operation Conventions

Convention	Purpose	Operation
Bold	The purpose of bolded text is used to alert the reader that additional text has been added to the CC requirement. Example: The TSF shall export **(in ASCII format)** the **labeled** user data's associated security attributes.	Assignment Refinement
Italics	The purpose of italicized text is to inform the reader of an assignment or selection operation to be completed by the developer. Example: The TSF shall provide the following [*ST Assignment: list of additional SFP capabilities*].	Assignment Selection
Parentheses	The purpose of using parentheses and an iteration number is to inform the reader that the author has selected a new field of assignments or selections with the same requirement and that the requirement will be used multiple times.	Iteration
<u>Underline</u>	The purpose of underlined text is to inform the reader that a choice was made from a list provided by the CC selection operation statement. Example: The TSF shall be able to <u>prevent</u> modifications to the audit records.	Selection

Application notes provide support information that is considered relevant or useful for the construction, evaluation, or use of the Target of Evaluation (TOE). Application notes clarify the intent of a requirement, identify implementation choices, or define "pass-fail" criteria for a requirement. Application notes follow the relevant requirement component, are directive in nature, and may amplify the CC terminology stated in a specific requirement.

1.3.2 Naming Conventions

Assumptions: TOE security environment assumptions are given names beginning with "A." e.g., A.COMPONENTS.

Threats: TOE security environment threats are given names beginning with "T." e.g., T.IMPORT.

Policies: TOE security environment policies are given names beginning with "P." e.g., P.COMPLY.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE." respectively e.g., O.DATA_PRO and OE.EMAIL.

1.4 Glossary of Terms

This profile uses the terms described in this section to aid in the application of the requirements:

Authorized user	A user who has been uniquely identified and authenticated. These users are considered to be legitimate users of the TOE.

1.5 Document Organization

Section 1 provides the introductory material for the PP.

Section 2 describes the Handheld (i.e. the TOE for this PP) and its general purpose.

Section 3 describes the expected environment for the Handheld. This section defines:

- Secure use assumptions that describe the presumptive conditions for secure use in the selected environment,
- Threats that are to be addressed by either the technical countermeasures implemented in the Handheld hardware or software or through the environmental controls, and
- Organizational policies that levy further requirements for secure operations.

Section 4 defines the security objectives for both the Handheld and its environment.

Section 5 contains the functional and assurance requirements derived from the CC, Parts 2 and 3, respectively, that must be satisfied by the Handheld technology and development teams, respectively.

Section 6 provides a rationale to demonstrate explicitly that the information technology security objectives satisfy the policies and threats. Arguments are provided for the security objectives being necessary to support policies and counter threats. The section then explains how the set of requirements are sufficient to meet each objective, and that each security objective is addressed by one or more component requirements. Therefore, the two aforementioned subsections provide arguments that the security objectives and security requirements are both necessary and sufficient, respectively and collectively, to meet the needs dictated by the policies and threats. Next, Section 6 provides arguments that address strength of function issues, choice of assurance requirements, and the use of explicitly stated requirements.

An acronym list is provided to define frequently used acronyms.

The reference section identifies background material used to prepare this PP.

2 TOE Description

The wireless two-way email solution provides a security enhanced electronic mail messaging solution for the remote monitoring, creation and distribution of mail messages. The two-way wireless e-mail solution includes several related components. They are the Handheld device, the Mail Server Interface, and the Desktop with docking cradle. Figure 1, Wireless Two-way Email Architecture Components, illustrates the relationships between the components. The Handheld device is a mobile device that allows users to receive, review, and send email messages remotely. The Mail Server Interface is responsible for administering policy for the users and devices and properly distributing email to and from the handheld. The Desktop and cradle provide the user with the functionality to synchronize the desktop mailbox with the handheld and to download approved software and policies. Features of the wireless two-way email solution include:

- A single email address such that a message sent from the handheld and a message sent from the desktop is not distinguishable.
- A protected end-to-end transmission link between the handheld and the protected enclave where the server and desktop are located.
- Use of S/MIME to provide secure mail messaging for sensitive but unclassified email.

Each component is specified in a separate PP and thus is a separate Target of Evaluation (TOE). Specifically, the TOE for this PP is the Handheld. The TOE includes all software and hardware components that encompass the Handheld. The Mail Server and Desktop, as well as the communications network, are not part of the TOE and considered part of the information technology (IT) environment.

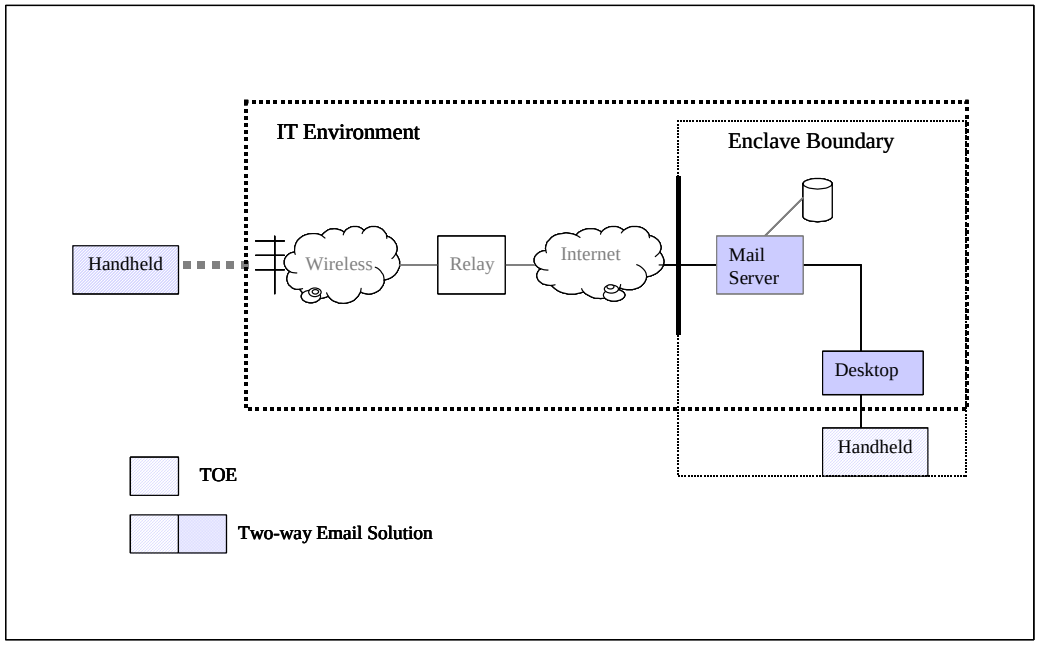

Figure 1 Wireless Two-way Email Architecture Components

The Handheld is a single-user medium assurance device. The configuration of the Handheld is controlled by policies defined by the server, and applications, information (e.g., address books, certificates) downloaded from and synchronized with the desktop. The Handheld shall provide the following security services in its evaluated TOE configuration:

Identification and Authentication – the user must provide I&A data prior to accessing any applications or email messages on the handheld device. The TOE provides the capability to support two forms of authentication, card authentication and password authentication. The TOE stores any handheld passwords that are used as part of authentication in an unreadable form. When a smartcard reader is present as part of the handheld, the TOE forces the user to perform card authentication. The TOE enforces several restrictions on authentication data including, password length, strength, and character set. The TOE also provides a lockout capability, which locks the handheld and removes useful data after the user has entered an administrator-determined, number of invalid attempts.

Self-Protection – The TOE provides domain separation and non-bypassability protection. The TOE contains only approved and signed software. All other information on the Handheld is treated as data and is not considered executable. The device itself must be protected from physical tampering by methods similar to tamper resistant seals.

Data Protection – The TOE provides the capability to create, read, and send signed and/or encrypted S/MIME mail messages using class 3 or 4, X.509 certificates. The security of the S/MIME mail messages includes authentication of the user, confidentiality and integrity of the message body and envelope, and non-repudiation of the originator. No encrypted S/MIME mail messages are stored in plaintext on the handheld. The TOE supports plaintext (non-S/MIME) mail messages to be sent and received by the handheld. All mail messages are encrypted for transmission over the communication network using, at a minimum, a FIPS-140-1 (Level 1) approved algorithm/cryptographic module.

3 TOE Security Environment

The laws, organizational security policies, customs, expertise and knowledge that are relevant to the TOE define the security environment. The purpose of this section is to describe the nature and scope of security in which the TOE is intended to be used. The security environment is captured by security specific statements made about the TOE in terms of assumptions, threats, and applicable organizational security policies.

Subsequent sections of the PP and ST show how the TOE, in combination with its operating environment, will address the security environment.

3.1 Secure Usage Assumptions

This section discusses the scope of intended usage of the TOE as well as assumptions about the operating environment including physical, personnel, and connectivity issues.

Table 2 TOE Assumptions

Name	Assumption
A.COMPONENTS	The server and desktop operate within a protected enclave that provides protection against tampering and unauthorized physical access.
A.EMAIL	The TOE is capable of receiving and transmitting plaintext mail messages.
A.ENVIRON	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
A.IT_ENVIRON	The IT environment of the TOE does not contain vulnerabilities that undermine the secure operation of the TOE.
A.TRAIN	Users are trained on the proper operations and procedures of the TOE.
A.PKI	Within the IT environment, there is a PKI that provides valid class 3 or 4, X.509 certificates.

3.2 Threats to Security

The TOE will provide protection against the threats listed in Table 3. These threats are actions that may have an adverse affect on the Handheld or its mission.

Table 3 Threats

Name	Threat
T.EAVESDROPPING	An unauthorized user reads sensitive but unclassified email by monitoring communications to and from the

	TOE and the server.
T.HACK_MSG_CONTENT	A hacker modifies information intercepted from the RF or wired communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient.
T.IMPORT	An administrator or user may import malicious code to the system, resulting in a compromise of the integrity and/or availability of the TOE.
T.SPOOFING	An attacker masquerades as a valid user to deliver spurious email.
T.UNAUTH_ACCESS	An unauthorized user gains access to the TOE due to weak authentication controls.

3.3 Organizational Security Policies

Organizational security policies define a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 4 identifies the organizational security policies applicable to the Handheld.

Table 4 Organizational Security Policies

Name	Policy
P.COMPLY	The implementation and use of the TOE must comply with all applicable laws, regulations, and guidelines imposed on the organization.
P.CRYPTO	Encryption used to protect transmitted user data and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1).
P.DEDICATED	The TOE must be used for only purposes as specified by the organization.
P.GUIDANCE	Guidance must be provided for the secure installation and use of the system.
P.KNOWN	Users of the TOE must be identified and authenticated before access to TOE functions can be granted.
P.PKI	DOD Class 3 or 4, Version 3 X.509 certificates shall be used as appropriate for encryption and to digitally sign email.[1]
P.PASSWORD	Password based authentication mechanism must support a password space that allows alphanumeric, upper and lower case enforced symbols, a minimum password length of 8, and a feature to limit failed login attempts. Passwords shall not be echoed in a readable format.
P.NO_TAMPER	The TOE must protect itself from physical tampering.

[1] Certificates used shall be consistent with the DOD PKI release in effect or planned.

P.SMIME	S/MIME messaging application used by the TOE must be PKI-enabled and compliant with S/MIME version 3.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 5 identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified.

Table 5 Security Objectives for the TOE

Name	TOE Security Objective	Corresponding Threat or Policy
O.DATA_PRO	The TOE shall use cryptographic modules compliant at a minimum with FIPS 140-1 (Level 1) to provide confidentiality and integrity of user data in transit between the TOE and the server.	P.CRYPTO T.EAVESDROPPING T.HACK_MSG_CONTENT
O.DOC	Guidance documentation provided to authorized users and administrators will detail the proper installation and use of the TOE to minimize the security risks within its intended environment.	P.GUIDANCE
O.EAL	The TOE must be structurally tested, shown to be resistant to vulnerabilities, and be documented with sufficient design, test, configuration, and lifecycle documentation.	P.COMPLY
O.IDENTITY	The TOE shall uniquely identify and authenticate each user of the system. The TOE shall not allow any user actions to be performed before the TOE verifies the identity of the user.	P.KNOWN
O.PASSWORD	The TOE will use an authentication mechanism that cannot be easily compromised in a moderate threat environment.	T.UNAUTH_ACCESS P.PASSWORD

Name	TOE Security Objective	Corresponding Threat or Policy
O.PROTECT_MAIL	The TOE shall control access to and protect encrypted S/MIME mail messages from disclosure. S/MIME mail messages created and processed shall be compliant with S/MIME version 3.	P.PKI P.SMIME T.SPOOFING T.HACK_MSG_CONTENT
O.VALID_CODE	The TOE must protect itself from unauthorized modification and access to its functions and data. TOE generation shall successfully validate all software updates before execution.	T.IMPORT P.DEDICATED

4.2 Security Objectives for the Environment

The assumptions identified in Section 3.1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 6 identifies the security objectives for the environment.

Table 6 Security Objectives for the Environment

Name	Security Objective	Corresponding Assumption, Threat, or Policy
OE.COMPONENTS	Those responsible for the TOE must ensure the server and desktop operate within a protective enclave.	A.COMPONENTS
OE.DEDICATED	Those responsible for the TOE must identify approved applications and software for the TOE to ensure that the TOE is used only for defined purposes.	P.DEDICATED P.COMPLY
OE.EMAIL	Those responsible for the TOE will allow the TOE to send and receive plaintext mail messages (non-S/MIME mail messages).	A.EMAIL

Name	Security Objective	Corresponding Assumption, Threat, or Policy
OE.IT_ENVIRON	Those responsible for the TOE must ensure the TOE is used within an IT environment that does not contain vulnerabilities to undermine the secure operation of the TOE. Only approved network providers per organizational regulations shall be used.	A.IT_ENVIRON
OE.MED_EXP	Those responsible for the TOE must ensure the TOE is used in an environment in which the threat of malicious attacks is no more than moderate.	A.ENVIRON P.COMPLY
OE.NO_TAMPER	Those responsible for the TOE will apply tamper resistant seals to the TOE to allow visual detection of physical tampering.	P.NO_TAMPER
OE.TRAIN	Users are trained on the proper operations and procedures of the TOE to include proper security protection for sensitive messages (sign, encrypt, verify signature).	A.TRAIN T.SPOOFING
OE.PKI	Those responsible for the TOE will ensure the TOE uses a PKI that provides valid class 3 or 4, Version 3 X.509 certificates.	A.PKI

5 IT Security Requirements

This section provides functional and assurance requirements that must be satisfied by a PP-compliant TOE. These requirements consist of functional components from Part 2 of the Common Criteria (CC) and an EAL containing assurance components from Part 3 of the CC.

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section provides information related to the TOE's Security Functional Requirements (SFRs). The first subsection addresses strength of function claims. The second subsection identifies standards compliance methods for the cryptographic SFRs included in this PP. The third subsection specifies the SFRs.

5.1.1 STRENGTH OF FUNCTION CLAIMS

The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism, except for cryptographic functions. In the case of this protection profile, this minimum level shall be SOF-Medium.

Specific strength of function (SoF) metric is defined for the authentication mechanism defined in FIA_UAU.1 and FIA_UAU.5. Strength of function shall be demonstrated for the authentication mechanism such that for each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000.

5.1.2 TOE Security Functional Requirements

The SFRs for the TOE consist of the following components from Part 2 of the CC summarized in Table 7.

Table 7 TOE Security Functional Requirements

Functional Component		Dependencies
FCS_COP.1	Cryptographic operation	FDP_ITC.1 or FCS_CKM.1; FCS_CKM.4; FMT_MSA.2
FDP_ACC.1(1)	Subset access control	FDP_ACF.1
FDP_ACF.1(1)	Security attribute based access control	FDP_ACC.1; FMT_MSA.3
FDP_ACC.1(2)	Subset access control	FDP_ACF.1
FDP_ACF.1(2)	Security attribute based access control	FDP_ACC.1; FMT_MSA.3
FDP_RIP.1	Subset residual information protection	None
FDP_UCT.1	Basic data exchange confidentiality	FTP_ITC.1 or FTP_TRP.1; FDP_ACC.1 or FDP_IFC.1
FDP_UIT.1	Data exchange integrity	FTP_ITC.1 or FTP_TRP.1; FDP_ACC.1 or FDP_IFC.1
FIA_AFL.1	Authentication failure handling	FAU_UAU.1
FIA_UAU.1	Timing of authentication	FIA_UID.1
FIA_UAU.5	Multiple authentication mechanisms	None
FIA_UAU.7	Protected authentication feedback	FIA_UAU.1
FIA_UID.1	Timing of identification	None
FMT_MSA.1(1)	Management of security attributes	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1
FMT_MSA.1(2)	Management of security attributes	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1
FMT_SMR.1(1)	Security Roles	FIA_UID.1
FPT_ITC.1	Inter-TSF confidentiality during transmission	None
FPT_SEP.1	TSF domain separation	None
FPT_RVM.1	Non-bypassability of the TSP	None
FTP_ITC.1(1)	Inter-TSF trusted channel	None
FTP_ITC.1(2)	Inter-TSF trusted channel	None

5.1.2.1 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform **encryption of server connections** in accordance with a specified cryptographic algorithm [*ST Assignment: cryptographic algorith*m] and cryptographic key sizes [*ST Assignment: cryptographic key size*s] that meet the following: **FIPS PUB 140-1 (Level 1) standard or FIPS 140-2 (Level 1) standard.**

Dependencies:
[FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

APPLICATION NOTE: This requirement is included to support the need to protect email sent to and received from the handheld. Encryption shall be used to ensure the integrity and confidentiality of all data transmitted from the handheld to the Mail Server. The intent of this requirement is not for the evaluator to perform a FIPS PUB 140-1 or FIPS PUB 140-2 evaluation; rather, the evaluator will check for a certificate, verifying that the module did complete a FIPS PUB 140-1 or FIPS PUB 140-2 evaluation.

5.1.2.2 FDP_ACC.1(1) Subset access control

Hierarchical to: No other component.

FDP_ACC.1.1(1) The TSF shall enforce the **plaintext email access control policy** on **individual plaintext mail messages, S/MIME mail messages, and users, and mail operations among users and mail messages covered by the plaintext email access control policy**.

Dependencies:
FDP_ACF.1 Security attribute based access control

APPLICATION NOTE: This requirement establishes the policy to allow the handheld to support other mail applications in addition to S/MIME. These mail applications do not provide protection from disclosure or modification.

5.1.2.3 FDP_ACC.1(2) Subset access control

Hierarchical to: No other component.

FDP_ACC.1.1(2) The TSF shall enforce the **secure email access control policy** on **individual S/MIME mail messages and users, and mail operations among users and mail messages covered by the secure email access control policy**.

Dependencies:
FDP_ACF.1 Security attribute based access control

APPLICATION NOTE: This requirement establishes the policy for the handheld to use S/MIME mail applications for sensitive but unclassified mail messages. S/MIME mail provides confidentiality and integrity protection.

5.1.2.4 FDP_ACF.1(1) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(1) The TSF shall enforce the **plaintext email access control policy** to objects based on **authenticated handheld user identity**.

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) **authenticated handheld user will be granted full access to their plaintext mail messages**,
b) **Authenticated handheld user will be granted read access to their signed only S/MIME mail messages**,
c) [*ST Assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled object*s].

FDP_ACF.1.3(1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*ST Assignment: rules, based on security attributes, that explicitly authorize access of subjects to object*s].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the [*ST Assignment: rules, based on security attributes, that explicitly deny access of subjects to object*s].

Dependencies:
FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

APPLICATION NOTE: This requirement in conjunction with FDP_ACC.1(1) establishes the policy to allow the handheld to support other mail applications in addition to a S/MIME mail application. The user is required to logon to the handheld before accessing plaintext mail messages and signed S/MIME mail messages. An unsigned S/MIME message is considered to be a plaintext mail message.

5.1.2.5 FDP_ACF.1(2) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(2) The TSF shall enforce the **secure email access control policy** to objects based on **authenticated handheld user identity and authenticated key store user identity**.

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) Authenticated handheld user is granted read access to encrypted S/MIME mail message if key store authentication is successful,

b) Authenticated handheld user is granted write access to create a S/MIME mail message with signature if key store authentication is successful

c) Authenticated handheld user is granted write access to create a S/MIME mail message with encryption if key store authentication is successful and

d) [*ST Assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled object*s].

FDP_ACF.1.3(2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*ST Assignment: rules, based on security attributes, that explicitly authorise access of subjects to object*s].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the [*ST Assignment: rules, based on security attributes, that explicitly deny access of subjects to object*s].

Dependencies:
FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

APPLICATION NOTE: This requirement in conjunction with FDP_ACC.1(2) establishes the policy for the handheld to use S/MIME mail applications for sensitive but unclassified mail messages. In addition to logging into the handheld, the user is required to authenticate themselves before decrypting S/MIME mail messages. The user is required to authenticate themselves before signing and/or encrypting S/MIME mail messages. Note that encrypting an email message includes applying a signature.

5.1.2.6 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: **S/MIME mail messages**.

Dependencies: No dependencies

5.1.2.7 FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the **plaintext email access control policy and secure email access control policy** to be able to transmit, and receive objects in a manner protected from unauthorized disclosure.

Dependencies:
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

APPLICATION NOTE: This requirement captures the need to protect email sent to and received from the handheld. Encryption shall be used to ensure the confidentiality of email messages in transmission.

5.1.2.8 FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the **plaintext email access control policy and secure email access control policy** to be able to transmit and receive user data in a manner protected from modification errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification has occurred.

Dependencies:
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

APPLICATION NOTE: This requirement captures the need to protect email sent to and received from the handheld. Encryption shall be used to ensure the integrity of email messages in transmission.

5.1.2.9 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when **configurable number of** unsuccessful authentication attempts occur related to **handheld logons.**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **render the handheld unusable.**

Dependencies:
FIA_UAU.1 Timing of authentication

APPLICATION NOTE: This requirement captures the need to restrict the number of failed login attempts to the handheld. The handheld should be put in an unusable state (e.g., reverted back to manufacturer default settings) when the limit of consecutive unsuccessful logon attempts has been reached.

5.1.2.10 FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that **reusable password** secrets meet **the following quality metric:**

a) password secret is composed of alphanumeric, upper and lower case characters;
b) password secret contains at least one special character and one numerical character;
c) password secret length is at a minimum 8 symbols;
d) password is not within the predefined number of previously used passwords; and
e) password meets global password policy.

Dependencies: No dependencies

APPLICATION NOTE: This requirement applies when the user is changing their password. This requirement establishes the minimum quality metric that must enforced. The Mail Server can set a global password policy which is downloaded to the Handheld. The global password policy must also satisfy the minimum quality metric.

5.1.2.11 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow **no actions** on behalf of the user to be performed before the user is authenticated **to the handheld**.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies:
FIA_UID.1 Timing of identification

5.1.2.12 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide **password handheld authentication and key store authentication mechanisms** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **following multiple authentication mechanism rules:**

a) reusable password handheld mechanism shall be used for users to access the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that user.

b) Reusable password handheld mechanism shall not allow access to the TOE if the password has expired.

c) Key store authentication mechanism shall be used for users to process S/MIME mail messages such that successful authentication must be achieved before allowing operations to be performed on behalf of the user as specified in FDP_ACF.1(2).

Dependencies: No dependencies

APPLICATION NOTE: This requirement defines two types of authentication mechanism that is required to access the TOE and S/MIME mail messages. The user must be authenticated before doing anything on the handheld. If the user enters a password that has expired, the user is denied access to the TOE. Stored S/MIME messages are encrypted and cannot be read unless the user provides the appropriate password for the key store of certificates. The creation of a signed or encrypted message also requires the user to provide the appropriate password for the key store. Certificates can be stored in software or on a hardware token (e.g., CAC). The TOE must authenticate the user before allowing use of certificates (i.e., key store authentication).

5.1.2.13 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only **feedback that does not divulge authentication data** to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

5.1.2.14 FIA_UID.1 Timing of Identification

Hierarchical to: No other components

FIA_UID.1.1 The TSF shall allow **no actions** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.2.15 FMT_MSA.1(1) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(1) The TSF shall enforce the **plaintext email access control policy** to restrict the ability to modify the security attributes **handheld password** to **the authorized user**.

Dependencies:
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

5.1.2.16 FMT_MSA.1(2) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(2) The TSF shall enforce the **secure email access control policy** to restrict the ability to modify the security attributes **key store password** to **the authorized user.**

Dependencies:
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

5.1.2.17 FMT_SMR.1(1) Security roles

Hierarchical to: No other components.

FMT_SMR.1.1(1) The TSF shall maintain the **role authorized user**.

FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

APPLICATION NOTE: This requirement is included to satisfy a dependency for FMT_MSA.1. The TOE trivially meets this requirement because the TOE is a single-user device. Once the user is authenticated to the handheld, the user becomes an authorized user.

5.1.2.18 FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Dependencies: No dependencies

5.1.2.19 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.1.2.20 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

APPLICATION NOTE: The TOE must provide a security architecture such that all the functionality described by the TOE requirements in this PP cannot be bypassed. This means that the TOE should not have any external interfaces that can bypass the functionality described.

5.1.2.21 FTP_ITC.1(1) Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1(1) The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2(1) The TSF shall permit the TSF and the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for **transfer of mail messages.**

Dependencies: No dependencies

APPLICATION NOTE: The TOE interacts with the server to send and receive mail messages to/from the protected enclave (the user's desktop). This requirement supports the concept that connectivity to secure email components must be trusted and thus protected.

5.1.2.22 FTP_ITC.1(2) Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1(2) The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2(2) The TSF shall permit the TSF and the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for **configuration data, software updates, and certificates.**

Dependencies: No dependencies

APPLICATION NOTE: The TOE is configured from the desktop in which configuration data (e.g., symmetric keys, policy settings), certificates, CRLs, and software applications are downloaded to the handheld. This requirement supports the concept that connectivity to secure email components must be trusted and thus protected.

5.1.3 Security Requirements for the IT Environment

This section identifies the IT security requirements that are to be met by the IT environment of the TOE (i.e., CAC, Server, desktop). The requirements identified in Table 8 are not all inclusive of the security requirement that the IT environment must satisfy but rather are those requirements in which the TOE depends upon for its correct operation. It should be noted that where security requirements for the IT environment

refer to the TSF, they refer to the security functions of the environment not security functions of the TOE.

Table 8 Security Requirements for the IT Environment

Functional Component		Dependencies
FCS_COP.1 (Mail Server)	Cryptographic operation	FDP_ITC.1 or FCS_CKM.1; FCS_CKM.4; FMT_MSA.2
FTP_ITC.1 (Mail Server) (Desktop)	Inter-TSF trusted channel	None
FPT_ITC.1 (Mail Server)	Inter-TSF confidentiality during transmission	None
FIA_UAU.1 (smart card)	Timing of authentication	FIA_UID.1
FMT_MTD.1 (Mail Server)	Management of TSF data	FMT_SMR.1
FMT_SMR.1 (2) (Mail Server)	Security Roles	None

5.2 TOE Security Assurance Requirements

The TOE security assurance requirements, summarized in Table 9, detail the evidence and evaluation activities required for the Handheld to be used in the security environment described in this protection profile. Section 6 provides a justification for the chosen security assurance requirements and the selected EAL 4 assurance level.

Table 9 TOE Assurance Requirements

Assurance Class	Assurance Components
Configuration Management	Partial CM automation (ACM_AUT.1) Generation support and acceptance procedures (ACM_CAP.4) Problem tracking CM coverage (ACM_SCP.2)
Delivery and Operations	Detection of modification (ADO_DEL.2) Installation, generation, and start-up procedures (ADO_IGS.1)
Development	Fully defined external interfaces (ADV_FSP.2) Security enforcing high-level design (ADV_HLD.2) Subset of the implementation of the TSF (ADV_IMP.1) Descriptive low-level design (ADV_LLD.1)

Assurance Class	Assurance Components
	Informal correspondence demonstration (ADV_RCR.1)
	Informal TOE security policy model ((ADV_SPM.1)
Guidance documents	Administrator guidance (AGD_ADM.1)
	User guidance (AGD_USR.1)
Life cycle support	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Well-defined development tools (ALC_TAT.1)
Tests	Analysis of coverage (ATE_COV.2)
	Testing: high-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing - sample (ATE_IND.2)
Vulnerability Assessment	Validation of analysis (AVA_MSU.2)
	Strength of TOE security function evaluation (AVA_SOF.1)
	Independent vulnerability analysis (AVA_VLA.2)

5.2.1 Partial CM automation (ACM_AUT.1)

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements:

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements:

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Generation support and acceptance procedures (ACM_CAP.4)

Dependencies:

ACM_SCP.1 TOE CM coverage
ALC_DVS.1 Identification of security measures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a Configuration Management (CM) system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labelled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action items:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3 Problem tracking CM coverage (ACM_SCP.2)

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements:

ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Detection of modification (ADO_DEL.2)

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements:

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action items:

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Installation, generation, and start-up procedures (ADO_IGS.1)

Dependencies:

AGD_ADM.1 Administrator guidance

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS_EXP.1.2C The generation procedures shall include a software validation step in which the TSF shall perform a software validation operation to verify the authenticity and integrity of executables.

Evaluator action items:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.6 Fully defined external interfaces (ADV_FSP.2)

Dependencies:

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action items:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.7 Security enforcing high-level design (ADV_HLD.2)

Dependencies:

ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality pro-vided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action items:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.8 Subset of the implementation of the TSF (ADV_IMP.1)

Dependencies:

ADV_LLD.1 Descriptive low-level design
ADV_RCR.1 Informal correspondence demonstration
ALC_TAT.1 Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.2.9 Descriptive low-level design (ADV_LLD.1)

Dependencies:

ADV_HLD.2 Security enforcing high-level design
ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements:

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.10 Informal correspondence demonstration (ADV_RCR.1)

Dependencies:

No dependencies.

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action items:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

APPLICATION NOTE: For this PP, this applies to ensure that the TOE summary specification contained in the Security Target and functional specification, functional specification and high-level design, high-level design and low-level design, and low-level design and implementation representation are consistent with each other.

5.2.11 Informal TOE security policy model (ADV_SPM.1)

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:
ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.12 Administrator guidance (AGD_ADM.1)

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documents supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

Evaluator action items:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.13 User guidance (AGD_USR.1)

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces avail-able to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

Evaluator action items:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.14 Identification of security measures (ALC_DVS.1)

Dependencies:
No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.2.15 Developer defined life-cycle model (ALC_LCD.1)

Dependencies:
No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.16 Well-defined development tools (ALC_TAT.1)

Dependencies:

ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements:

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.17 Analysis of coverage (ATE_COV.2)

Dependencies:

ADV_FSP.1 Informal functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action items:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.18 Testing: high-level design (ATE_DPT.1)

Dependencies:

ADV_HLD.1 Descriptive high-level design
ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

ATE_DPT.1.2E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.19 Functional testing (ATE_FUN.1)

Dependencies:
No dependencies.

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action items:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.20 Independent testing - sample (ATE_IND.2)

Dependencies:

ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action items:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

APPLICATION NOTE: The choice of the subset tested and the sample tests executed is entirely at the discretion of the evaluator.

5.2.21 Validation of analysis (AVA_MSU.2)

Dependencies:

ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.2.22 Strength of TOE security function evaluation (AVA_SOF.1)

Dependencies:

ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive high-level design

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the Security Target (ST) as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action items:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

APPLICATION NOTE: For this protection profile, this requirement applies to the authentication mechanism described for FIA_UAU.1.

5.2.23 Independent vulnerability analysis (AVA_VLA.2)

Dependencies:

ADV_FSP.1 Informal functional specification
ADV_HLD.2 Security enforcing high-level design
ADV_IMP.1 Subset of the implementation of the TSF
ADV_LLD.1 Descriptive low-level design
AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements:

AVA_VLA.2.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.2.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.2.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Evaluator action elements:

AVA_VLA.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

6 Rationale

This section provides the rationale for the selection, creation, and use of security objectives and requirements.

6.1 Security Objectives Rationale

The security objectives rationale demonstrates that the stated security objectives (in Section 4) are traceable to all of the aspects identified in the TOE security environment (described in Section 3) and are suitable to cover them.

Table 5 in Section 4 shows that all security objectives for the TOE are traced back to aspects of the identified threats (in Section 3.2) and/or aspects of the organizational security policies to be met by the TOE (in Section 3.3). Table 6 in Section 4.0 shows that all security objectives for the environment are traced back to aspects of the organizational security policies and/or assumptions to be met by the TOE's environment. Table 10 presents the justification that the security objectives are suitable to counter the threats, and cover the OSP and assumptions described in Section 3.

Table 10 Security Objectives Justification

Threat/OSP/Assumption	Security Objective(s)	Justification
T.EAVESDROPPING	O.DATA_PRO	*An unauthorized user reads sensitive but unclassified email by monitoring communications to and from the TOE and the server.* O.DATA_PRO requires the use of encryption to protect transmitted email from disclosure.

Threat/OSP/Assumption	Security Objective(s)	Justification
T.HACK_MSG_CONTENT	O.DATA_PRO, O.PROTECT_MAIL	*A hacker modifies information intercepted from the RF or wired communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient.* Both O.DATA_PRO and O.PROTECT_MAIL provide for the use of encryption to detect when information has been modified. O.DATA_PRO is concerned with encrypting the mail in transmission; O.PROTECT_MAIL is concerned with encrypting the mail message itself by using S/MIME.
T.IMPORT	O.VALID_CODE	*An administrator or user may import malicious code to the system, resulting in a compromise of the integrity and/or availability of the TOE.* O.VALID_CODE levies requirements on the TOE to protect itself to include validating all software updates before execution. This validation will only allow the use of authorized code for the handheld and avoid the insertion of malicious code.
T.SPOOFING	O.PROTECT_MAIL OE.TRAIN	*An attacker masquerades as a valid user to deliver spurious email.* O.PROTECT_MAIL allows for the use of S/MIME which supports digital signatures to verify the source of messages. OE.TRAIN requires the user to be properly trained to recognize the potential threat of receiving malicious or fraudulent email.

Threat/OSP/Assumption	Security Objective(s)	Justification
T.UNAUTH_ACCESS	O.PASSWORD	*An unauthorized user gains access to the TOE due to weak authentications controls.* O.PASSWORD levies requirements to provide a strong authentication mechanism strong enough for the intended environment.
P.COMPLY	O.EAL OE.DEDICATED OE.MED_EXP	*The implementation and use of the TOE must comply with all applicable laws, regulations, and guidelines imposed on the organization.* O.EAL levies requirements on the TOE development and evaluation to be consistent with its intended use as prescribed by this PP. OE.DEDICATED is concerned with having the TOE only execute approved applications and OE.MED_EXP ensures that the TOE is only used in the intended environment and not for higher risk environments for which it was not designed.
P.CRYPTO	O.DATA_PRO	*Encryption used to protect transmitted user data and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1).* O.DATA_PRO levies the use of cryptographic modules which are compliant with at a minimum FIPS 140-1 (Level 1).
P.DEDICATED	O.VALID_CODE OE.DEDICATED	*The TOE must be used for only purposes as specified by the organization.* O.VALID_CODE levies requirements to only allow the use of authorized code for the handheld. OE.DEDICATED is concerned with having the TOE only execute

Threat/OSP/Assumption	Security Objective(s)	Justification
		approved applications
P.GUIDANCE	O.DOC	*Guidance must be provided for the secure installation and use of the system.* O.DOC provides the guidance documentation required for proper installation, generation, and use of the TOE.
P.KNOWN	O.IDENTITY	*Users of the TOE must be identified and authenticated before access to TOE functions can be granted.* O.IDENTITY requires user identification and authentication, by the TOE before allowing access. O.IDENTITY does restrict the ability to perform actions before authentication.
P.PKI	O.PROTECT_MAIL	*DOD Class 3 or 4, Version 3 X.509 certificates shall be used as appropriate for encryption and to digitally sign email.* O.PROTECT_MAIL requires the use of S/MIME which uses PKI certificates to encrypt and sign email messages.
P.PASSWORD	O.PASSWORD	*Password based authentication mechanism must support a password space that allows alphanumeric, upper and lower case enforced symbols, a minimum password length of 8, and a feature to limit failed login attempts. Passwords shall not be echoed in a readable format.* O.PASSWORD levies requirements to provide a strong authentication mechanism strong enough for the intended environment.

Threat/OSP/Assumption	Security Objective(s)	Justification
P.NO_TAMPER	OE.NO_TAMPER	*The TOE must protect itself from physical tampering.* OE.NO_TAMPER requires the organization using the TOE to apply tamper resistant seals to visual detect physical tampering.
P.SMIME	O.PROTECT_MAIL	*S/MIME messaging application used by the TOE must be PKI-enabled and compliant with S/MIME version 3.* O.PROTECT_MAIL requires the use of S/MIME messages compliant with version 3.
A.COMPONENTS	OE.COMPONENTS	*The server and desktop operate within a protected enclave that provides protection against tampering and unauthorized physical access.* OE.COMPONENTS levies requirements on those responsible for the TOE to ensure the other components of the two-way email solution are protected.
A.EMAIL	OE.EMAIL	*The TOE is capable of receiving and transmitting plaintext mail messages.* OE.EMAIL allows the use of mail applications in addition to S/MIME mail applications.
A.ENVIRON	OE.MED_EXP	*The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.* OE.MED_EXP ensures that the TOE is only used in the intended environment and not for higher risk environments for which it was not designed.

Threat/OSP/Assumption	Security Objective(s)	Justification
A.IT_ENVIRON	OE.IT_ENVIRON	*The IT environment of the TOE does not contain vulnerabilities that undermine the secure operation of the TOE.* Through procedural means, OE.IT_ENVIRON objective requires the maintainers of the TOE to properly install, configure, and operate the IT environment.
A.TRAIN	OE.TRAIN	*Users are trained on the proper operations and procedures of the TOE.* OE.TRAIN ensures authorized users are trained on security features of the system and how to use those features to properly protect sensitive mail.
A.PKI	OE.PKI	*Within the IT environment, there is a PKI that provides valid class 3 or 4, X.509 certificates.* OE.PKI ensures that only X.509 certificates are used by the TOE.

6.2 Security Requirements Rationale

The security requirements rationale demonstrates that the set of security requirements (in Section 5) is suitable to meet and traceable to the security objectives (specified in Section 4). The set of IT security requirements are internally consistent because they were all derived from Part 2 and Part 3 of the CC, operations were performed in accordance to the CC, and the security requirements were chosen and written to apply to the same concepts expressed in the security objectives. The IT security requirements together form a mutually supportive whole because they were derived from the TOE security objectives, include FPT_RVM.1, and FPT_SEP.1 to prevent bypassing and unauthorized modification of the TSF, and include security management requirements to properly manage the security functions.

6.2.1 TOE Assurance Requirements

This protection profile has been developed for a medium robustness environment. Given consideration to best commercial practices for COTS products and assurance requirements for the various assurance levels, it was determined that EAL 4 achievable and the most appropriate. The operational environment restrictions assumed by this PP and the capabilities of the host implementations support the choice of an EAL 4 set of assurance requirements. The addition of one explicitly stated functional elements to ADO_IGS.1 is consistent and non-contradictory with the other ADO_IGS.1 functional elements. The additional element was added to explicitly require certain information to be documented for installation, generation, and startup of the TOE.

6.2.2 Strength of Function Rationale

The minimum strength of function level SOF-medium was chosen because the TOE environment assumes an environment in which the threat of malicious software attacks aimed at discovering exploitable vulnerabilities is considered moderate. The strength of metric established for the authentication mechanism described in FIA_UAU.1 and FIA_UAU.5 (reusable password mechanism) was defined to ensure the mechanism is of adequate strength to protect against authentication data compromise. FIA_SOS.1 defines password characteristics that support the strength of metric chosen. The strength of function level and metric chosen are consistent with the security objectives of the TOE because the security objectives are derived from the TOE environment, which describes a moderate risk environment.

6.2.3 Dependency Satisfaction

Functional component FCS_COP.1 depends on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction and FMT_MSA.2 Secure Security Attributes. Cryptographic modules must be FIPS PUB 140-1or FIPS PUB 140-2 compliant. If the cryptographic module is indeed compliant with these FIPS PUBs, then the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-1or FIPS PUB 140-2 compliant.

Functional component FDP_ACC.1 depends on FMT_MSA.3 Static attribute initialization. The plaintext email access control policy and the secure email access control policy do not enforce rules of operation based on security attributes, which have default values. The FMT_MSA.3 component is not applicable for the policies defined by this PP.

6.2.4 Traceability

Table 11 shows how the requirements for the TOE map to the security objectives.

Table 11 Mapping of Requirements to Security Objectives

Security Objectives / TOE Security Functional Requirements	O.DATA_PRO	O.DOC	O.EAL	O.IDENTITY	O.PASSWORD	O.PROTECT_MAIL	O.VAILD_CODE
FCS_COP.1	●						
FDP_ACC.1(1)	●						
FDP_ACC.1(2)	●					●	
FDP_ACF.1(1)	●						
FDP_ACF.1(2)	●					●	
FDP_RIP.1						●	
FDP_UCT.1	●					●	
FDP_UIT.1	●					●	
FIA_AFL.1					●		
FIA_UAU.1				●	●		
FIA_UAU.5				●	●		
FIA_UAU.7					●		
FIA_UID.1				●			
FMT_MSA.1(1)	●						
FMT_MSA.1(2)	●						
FMT_SMR.1(1)	●						
FPT_ITC.1	●						
FPT_SEP.1							●
FPT_RVM.1							●
FTP_ITC.1(1)	●						
FTP_ITC.1(2)	●						
AGD_ADM.1		●					
AGD_USR.1		●					
ADO_IGS.1		●					●
EAL 4 Assurance Requirements (See Table 9)			●				

6.2.5 Suitability

In this section each security requirement is shown to be suitable to satisfy the security objectives.

O.DATA_PRO

The TOE shall use cryptographic modules compliant at a minimum with FIPS PUB 140-1 (Level 1) to provide confidentiality and integrity of user data in transit between the TOE and the server.

The following requirements satisfy O.DATA_PRO by requiring encryption compliant with FIPS PUB 140-1 (Level 1), the TSF to protect plaintext and S/MIME mail messages from unauthorized disclosure and modification when transmitted and received: FCS_COP.1, FDP_UCT.1, FDP_UIT.1.

FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1(1), FDP_ACF.1(2), FMT_MSA.1(1), FMT_MSA.1(2), FMT_SMR.1(1), FPT_ITC.1, FTP_ITC.1(1), and FTP_ITC.1(2) are included to satisfy dependencies.

O.DOC

Guidance documentation provided to authorized users and administrators will detail the proper installation, generation, and use of the TOE to minimize the security risks within the environment.

AGD_ADM.1 requires that the TOE vendor prepare guidance documentation for the authorized administrator. AGD_USR.1 requires that the TOE vendor prepare guidance documentation for the user. ADO_IGS.1 specifies installation and generation procedures.

O.EAL

The TOE must be structurally tested, shown to be resistant to vulnerabilities, and be documented with sufficient design, test, configuration, and lifecycle documentation.

The Assurance requirements for EAL 4 listed in Table 9 require that the TOE be designed and tested to conform to EAL 4. The EAL 4 requirements satisfy the security objective for a structurally tested, shown to be resistant to vulnerabilities, and a documented TOE.

O.IDENTITY

The TOE shall uniquely identify and authenticate each user of the system. The TOE shall not allow any user actions to be performed before the TOE verifies the identity of the user.

FIA_UAU.1 and FIA_UID.1 require a user to identify and authenticate themselves to the handheld before any action can be taken. FIA_UAU.5 defines all the situations and restrictions for each type of authentication a user would encounter.

O.PASSWORD

The TOE will use an authentication mechanism that cannot be easily compromised in a moderate threat environment.

FIA_UAU.1 and FIA_UAU.5 require an authentication mechanism and identifies specific password strength. Strong authentication for a password based authentication mechanism requires the TSF to limit the number of attempts a user has to guess a password (FIA_AFL.1), and to keep the password hidden (FIA_UAU.7).

O.PROTECT_MAIL

The TOE shall control access to and protect encrypted S/MIME mail messages from disclosure. S/MIME mail messages created and processed shall be compliant with S/MIME version 3.

FDP_ACC.1(2) and FDP_ACF.1(2) define the TSF policy to protect and control access to the S/MIME messages and FDP_RIP.1 protects against encrypted S/MIME messages from being disclosed once the message resource has been allocated back to the system. FDP_UCT.1, FDP_UIT.1 require protection of the S/MIME mail messages from unauthorized disclosure and modification when transmitted and received.

O.VALID_CODE

The TOE must protect itself from unauthorized modification and access to its functions and data. TOE generation shall successfully validate all software updates before execution.

FPT_SEP.1 requires the TOE to protect itself by maintaining its own execution domain and protecting itself from external interference and tampering of TSF code and data structures from untrusted software (subjects). FPT_RVM.1 ensures that all actions required for policy enforcement are validated by the TSF and cannot be bypassed (compromised). ADO_IGS.1 documents the procedures and steps of the TOE that are required for software validation of software updates.

6.2.6 Explicit Requirements Rationale

The following extended requirements have been included in this PP because the Common Criteria requirements were found to be insufficient as stated to meet the needs of the desired TOE specified.

ADO_IGS_EXP.1.2C	Generation procedures shall include a software validation step in which the TSF shall perform a software validation operation to verify the authenticity and integrity of executables.

7 Acronyms

CC - Common Criteria
CM – Configuration Management
COTS – Commercial-Off-The-Shelf
DoD – Department of Defense
EAL - Evaluation Assurance Level
IT - Information Technology
NSA – National Security Agency
OS – Operating System
PP - Protection Profile
SF - Security Function
SFP - Security Function Policy
SFR – Security Functional Requirement
S/MIME – Secure Multipurpose Internet Mail Extensions
SOF - Strength of Function
SSO – Site Security Officer
ST - Security Target
TBD – To be determined
TOE - Target of Evaluation
TSC - TSF Scope of Control
TSF - TOE Security Functions
TSFI - TSF Interface
TSP - TOE Security Policy

8 References

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1. CCIMB-99-021, 032, 033. August 1999.
[2] Common Methodology for Information Technology Security Evaluation, Version 1.0, CEM-99/045, August 1999.
[3] Secure Messaging PP, Version 0.21, November 9, 2000
[4] Wireless Two-Way Electronic Mail Mail Server Protection Profile, Version 1.0, June 2002
[5] Wireless Two-Way Electronic Mail Desktop Protection Profile, Version 1.0, June 2002